Security Assessment Summary — itsecgames.com

Scope: Publicly accessible web endpoint (itsecgames.com / 31.3.96.40)

Key Findings

Category	*Finding*	*Risk*
Critical	Drupal 7 (EOL) detected via X-Generator header	High — Known RCE/SQLi/XSS CVEs, actively exploited in the wild
High	Expired/self-signed TLS certificate (web.mmebvba.com)	High — Browser trust broken, vulnerable to MITM
High	Exposed installation & documentation files (install.php, UPGRADE.txt, INSTALL*.txt)	High — Leaks sensitive system information, may allow configuration exploits
Medium	Missing security headers (HSTS, CSP, X-Content-Type-Options)	Medium — Clickjacking, MIME-type attacks, weaker security posture
Medium	Potential XSS vulnerability (PostNuke module)	Medium — Could compromise users' sessions
Medium	Exposed configuration files & robots.txt	Medium — Information leakage and attack-surface mapping
Low / Info	Server banners reveal Apache & Drupal 7 versions; SSH port observed	Informational — Aids attackers in targeting

SSL/TLS Assessment

- Protocol: **TLS 1.2**
- Cipher: **ECDHE-RSA-AES256-GCM-SHA384**
- Key size: 2048-bit RSA
- Certificate: self-signed, expired May 22, 2025, CN mismatch (web.mmebvba.com)

Impact: Public-facing services cannot be fully trusted; automated scanners and browsers will flag security issues.

Recommendations

1. Immediate removal/blocking of installer and upgrade files.
2. Install a valid TLS certificate for itsecgames.com and enable HSTS.
3. Harden Apache with missing security headers and disable unnecessary HTTP methods.
4. Restrict SSH access to trusted IPs with key-based authentication.
5. Plan migration from Drupal 7 to a supported CMS platform.
6. Conduct post-remediation scans to confirm fixes.

Overall Risk Posture: High — immediate mitigation is required to prevent exploitation of legacy CMS, exposed files, and expired TLS certificate.